Monday

9:30 – 12 Trustwave - Web Application Firewall Architecture

This will cover a multi-faceted approach to Architecture, Best Practices, and other details surrounding Firewall Architecture. Topics will include availability, benefits, mitigating attacks and advanced protection methods, best practices, notifications, auditing, backup, patches, white and black lists, blocking, operational workflows, and performance monitoring.

1:00 – 4 Trustwave - Web Application Firewall Best Practices

This session will introduce industry practices that will help protect your website in an efficient and effective manner

Tuesday

Visit the Enterprise Security Program Booth

Wednesday

10:15-11:00 Digital Security

Many components go into creating and maintaining an effective security program, including policies, standards, training, and best practices. Jayne Friedland Holland will talk about NIC's security culture and highlight the key components of its security program that promotes the protection of its business and government partners.

11:15-12:00 Creating Effective Security Training and Awareness Program

You've probably heard it said, "people are the weakest link in security" and there's a lot of truth in that. While security awareness programs are often required to meet compliance regulations, how do you create a program that goes beyond "I'll do it because I have to" to a program that engages users and makes an impact? How do you create a culture where people understand and want to be secure? This session will focus on how to make information security awareness programs interesting, fun and educational.

11:15-12:00 Tools of the Trade

There are many popular network security tools in use on SummitNet; vulnerability scanners (nessus), splunk, kali, nmap, omnipeek, WAF, wireshark, netscout, winscp, virtual box / vmware workstation, websense, proxy, etc. This session will explain these tools and how they are used on our network.

1:45-2:45 What is Splunk and What can it do for me

Slunk can monitor and analyze anything and everything, from customer clickstreams and transactions to security events amd network activity. Splunk aggregates system, network, and security data to enable analysis from end-to-end. From troubleshooting to optimizing, Splunk gives you a single interface for searching logs and correlating events so you can better understand, manage, and secure your environment. The first half will cover architecture, data onboarding, and data searching followed by a Q&A session.

3:00-4:00 Digital Forensics

A discussion about how the Digital Forensics services from both SITSD and DOJ can assist customers with both criminal and non-criminal investigations relating to both user activity and security incidents for the State of Montana. The panel will distinguish the boundaries in which SITSD and DOJ can perform Digital Forensics. SITSD's portion will share some information of the trends in malware seen on devices and provide some ideas on how to mitigate infections. Plenty of time will saved to allow questions to the panel.

Thursday

10:15-11:00 Starting with Security

Introduction to creating a security program with a focus on policies and basic, high impact, and steps to take for securing IT systems.

11:15 -12:00 Source Control Best Practices

Source Control overview and why SITSD offers this essential service with a focus on Subversion, SITSD'S hosted solution. Discussion on similarities and differences between Subversion and other source control products on the market such as Git and Team Foundation Server. Introductory topics will include backup and recovery, versioning, repository snapshots, team collaboration, conflict resolution, security and accountability. Also covered will be how SITSD's internal development team uses source control to manager agile iterations smoothly, efficiently and effectively. This will transition into advanced topics that include branching/merging and tagging.

1:45-2:45 Physical Points of Intrusion

Physical door security. How easy is it enter your "secure" areas physically? See how simple it may be, and cheap ways to secure.

3:00-4:00 Introduction to System Security Plans and Risk Assessments

This panel will focus on concepts related to implementing a risk management strategy that complies with State of Montana statutory law, State of Montana enterprise security policies, federal regulations, and industry best practices. Additionally, this panel will provide helpful example templates and working strategies from agency officers that have been using these concepts in actual practice.

3:00-4:00 Varonis – Protecting your information from the Inside Out

Target lost 40,000,000 records in a 2014 breach that cost them $148 million dollars. Ouch. They had lots of fancy tools watching the perimeter, but fell short when it came to securing insider access. Protecting against insider threats, whether malicious or accidental, is extremely difficult, especially when 71% of employees say that they have access to information that they aren't supposed to see. Join us for a live presentation where you will learn six tactics for preventing insider threats.

Friday

8:00-12:00 Department of Homeland Security – Cyber Table Top Exercise

Join us for an entertaining and education tabletop exercise led by the Department of Homeland Security. Lelia Sloane and Timothy McCabe will lead attendees through a cyber security scenario to gain valuable insight. State employees, Local government employees, and University employees will all find value in this post conference session that will wrap up the 12th Annual conference.